Listing of Claims

1. (Original) A method for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, the method comprising the steps of:

routing both inbound and outbound communications with target hosts which are associated with a secure network communication through the distribution processor; and

processing both inbound and outbound secure network communications at the distribution processor so as to provide network security processing of communications from the target host and network security processing of communications to the target host.

2. (Original) A method according to Claim 1, further comprising the steps of:

receiving at the distribution processor, network communications directed to the common network address; and

distributing the received network communications to selected ones of the target hosts so as to distribute workload associated with the network communications.

3. (Original) A method according to Claim 2, further comprising the steps of:

determining if the received network communications are secure network communications which are to be distributed to ones of the target hosts;

wherein the step of processing both inbound and outbound secure network communications at the distribution processor comprises the step of processing the received network communications so as to provide generic communications to the ones of the plurality of target hosts if the received network communications are secure network communications which are distributed to ones of the target hosts.

4. (Original) A method according to Claim 3, wherein the step of processing both inbound and outbound secure network communications further comprises the steps of:

receiving at the distribution processor communications from the ones of the target hosts which are associated with secure network communications; and

processing the received communications from the ones of the target hosts so as to provide network security for the communications from the ones of the target hosts.

5. (Original) A method according to Claim 4, wherein the communications received from the target hosts and the generic communications to ones of the plurality of target hosts are encapsulated in a generic routing format.

6. (Original) A method according to Claim 4, wherein the generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distribution processor and ones of the plurality of target hosts.

7. (Original) A method according to Claim 4, wherein the communications received from the target hosts at the distribution processor and the generic communications to ones of the plurality of target hosts from the distribution processor are communicated over trusted communication links.

8. (Original) A method according to Claim 4, further comprising the step of establishing common IP filters for communications encapsulated in a generic routing format at the distribution processor and the plurality of target hosts.

9. (Original) A method according to Claim 8, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

10. (Original) A method providing Internet Protocol Security (IPSec) communications from a network to a plurality of application instances executing on a cluster of data processing systems utilizing virtual Internet Protocol Address (VIPA) Distributor to provide a routing communication protocol stack which distributes connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, the method comprising the steps of:

receiving inbound IPSec communications to the DVIPA from the network at the routing communication protocol stack;

performing IPSec processing of the received inbound IPSec communications at the routing communication protocol stack to provide non-IPSec communications to a first target communication protocol stack associated with the received inbound IPSec communications;

receiving outbound non-IPSec communications associated with the DVIPA from a second target communication protocol stack at the routing communication protocol stack; and

performing IPSec processing on the received outbound non-IPSec communications at the routing communication protocol stack to provide outbound IPSec communications to the network corresponding to the received outbound non-IPSec communications.

11. (Original) A method according to Claim 10, wherein the target communication protocol stacks carry out the step of sending outbound communications associated with a connection utilizing IPSec which is routed through the routing communication protocol stack to the routing communication protocol stack for IPSec processing.

12. (Original) A method according to Claim 10, wherein the second target communication protocol stack further carries out the steps of:

determining if an outbound communication associated with a connection utilizing IPsec is routed through the routing communication protocol stack;

sending non-IPSec communications for the connection utilizing IPSec to the routing communication protocol stack if the connection utilizing IPsec is routed through the routing communication protocol stack; and

IPSec processing communications if the connection utilizing IPSec is not routed through the routing communication protocol stack.

13. (Original) A method according to Claim 10, where the routing communication protocol stack and the plurality of target communication protocol stacks communicate utilizing a trusted communication link.

14. (Original) A method according to Claim 13, wherein the cluster of data processing systems comprises a Sysplex and wherein the trusted communication link is a cross coupling facility of the Sysplex.

15. (Original) A method according to Claim 10, wherein the routing communication protocol stack further carries out the steps of:

encapsulating the IPSec processed communications in a generic routing encapsulation (GRE) formatted communication; and

sending the GRE formatted communication to the first target communication protocol stack over a trusted communication link;

wherein the step of receiving outbound non-IPSec communications from a second target communication protocol stack at the routing communication protocol stack comprises the step of receiving a GRE encapsulated communication from the second target communication protocol stack; and

wherein the step of performing IPSec processing on the received outbound non-IPSec communications at the routing communication protocol stack to provide outbound IPSec communications to the network corresponding to the received outbound non-IPSec communications comprises the steps of:

extracting a non-IPSec communication from the received GRE encapsulated communication; and

IPSec processing the extracted non-IPSec communication.

16. (Original) A method according to Claim 15, further comprising the steps of establishing common IP filters for GRE encapsulated communications at the routing communication protocol stack and the target communication protocol stacks.

17. (Original) A method according to Claim 16, wherein the common IP filters bypass IP filtering for inbound GRE encapsulated communications.

18. (Original) A method according to Claim 15, wherein the cluster of data processing systems comprises a Sysplex and wherein the routing communication protocol stack and the target communication protocol stacks communicate utilizing a cross coupling facility (XCF) of the Sysplex and wherein the GRE encapsulated communications include an XCF source address and an XCF destination address in an outer GRE header.

19. (Original) A method according to Claim 18, further comprising the steps of:

evaluating an IP address of a physical link over which a GRE encapsulated communication was received and an IP address in the received GRE encapsulated communication to determine if the received GRE encapsulated communication was received over an XCF link; and

discarding the received GRE encapsulated communication if the received GRE encapsulated communication was not received over an XCF link.

20. (Original) A system for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, comprising:

means for routing both inbound and outbound communications with target hosts which are associated with a secure network communication through the distribution processor; and

means for processing both inbound and outbound secure network communications at the distribution processor so as to provide network security processing of communications from the target host and network security processing of communications to the target host.

21. (Original) A system according to Claim 20, further comprising:

means for receiving at the distribution processor, network communications directed to the common network address; and

means for distributing the received network communications to selected ones of the target hosts so as to distribute workload associated with the network communications.

22. (Original) A system according to Claim 21, further comprising:

means for determining if the received network communications are secure network communications which are to be distributed to ones of the target hosts;

wherein the means for processing both inbound and outbound secure network communications at the distribution processor comprise means for processing the received network communications so as to provide generic communications to the ones of the plurality of target hosts if the received network communications are secure network communications which are distributed to ones of the target hosts.

23. (Original) A system according to Claim 22, wherein the step of processing both inbound and outbound secure network communications further comprises:

means for receiving at the distribution processor communications from the ones of the target hosts which are associated with secure network communications; and

means for processing the received communications from the ones of the target hosts so as to provide network security for the communications from the ones of the target hosts.

24. (Original) A system according to Claim 23, wherein the communications received from the target hosts and the generic communications to ones of the plurality of target hosts are encapsulated in a generic routing format.

25. (Original) A system according to Claim 23, wherein generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distributing processor and ones of the plurality of target hosts.

26. (Original) A system according to Claim 23, wherein the communications received from the target hosts and the generic communications to ones of the plurality of target hosts are communicated over trusted communication links.

27. (Original) A system according to Claim 23, further comprising means for establishing common IP filters for communications encapsulated in the generic routing format at the distributing processor and the plurality of target hosts.

28. (Original) A system according to Claim 27, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

29. (Original) A system providing Internet Protocol Security (IPSec) communications from a network to a plurality of application instances executing on a cluster of data processing systems utilizing virtual Internet Protocol Address (VIPA) Distributor to provide a routing communication protocol stack which distributes connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, comprising:

means for receiving inbound IPSec communications to the DVIPA from the network at the routing communication protocol stack;

means for performing IPSec processing of the received inbound IPSec communications at the routing communication protocol stack to provide non-IPSec communications to a first target communication protocol stack associated with the received inbound IPSec communications;

means for receiving outbound non-IPSec communications from a second target communication protocol stack at the routing communication protocol stack; and

means for performing IPSec processing on the received outbound non-IPSec communications at the routing communication protocol stack to provide outbound IPSec communications to the network corresponding to the received outbound non-IPSec communications.

30. (Original) A system according to Claim 29, wherein the target communication protocol stacks further comprise means for sending outbound communications associated with a connection utilizing IPSec which is routed through the routing communication protocol stack to the routing communication protocol stack for IPSec processing.

31. (Original) A system according to Claim 10, wherein the target communication protocol stacks further comprises:

means for determining if an outbound communication associated with a connection utilizing IPSec is routed through the routing communication protocol stack;

means for sending non-IPSec communications for the connection utilizing IPSec to the routing communication protocol stack if the connection utilizing IPSec is routed through the routing communication protocol stack; and

IPSec processing communications if the connection utilizing IPSec is not routed through the routing communication protocol stack.

32. (Original) A system according to Claim 29, where the routing communication protocol stack and the plurality of target communication protocol stacks communicate utilizing trusted communication link.

33. (Original) A system according to Claim 32, wherein the cluster of data processing systems comprises a Sysplex and wherein the trusted communication link is a cross coupling facility of the Sysplex.

34. (Original) A system according to Claim 29, wherein the routing communication protocol stack further carries out the steps of:

means for encapsulating the IPSec processed communications in a generic routing encapsulation (GRE) formatted communication; and

means for sending the GRE formatted communication to the first target communication protocol stack over a trusted communication link;

wherein the means for receiving outbound non-IPSec communications from a second target communication protocol stack at the routing communication protocol stack comprises means for receiving a GRE encapsulated communication from the second target communication protocol stack; and

wherein the means for performing IPSec processing on the received outbound non-IPSec communications at the routing communication protocol stack to provide outbound IPSec

communications to the network corresponding to the received outbound non-IPSec communications comprises:

means for extracting a non-IPSec communication from the received GRE encapsulated communication; and

means for IPSec processing the extracted non-IPSec communication.

35. (Original) A system according to Claim 34, further comprising means for establishing common IP filters for GRE encapsulated communications at the routing communication protocol stack and the target communication protocol stacks.

36. (Original) A system according to Claim 35, wherein the common IP filters bypass IP filtering for inbound GRE encapsulated communications.

37. (Original) A system according to Claim 34, wherein the cluster of data processing systems comprises a Sysplex and wherein the routing communication protocol stack and the target communication protocol stacks communicate utilizing a cross coupling facility (XCF) of the Sysplex and wherein the GRE encapsulated communications include an XCF source address and an XCF destination address in an outer GRE header.

38. (Original) A system according to Claim 37, further comprising:

means for evaluating an IP address of a physical link over which a GRE encapsulated communication was received and an IP address in the received GRE encapsulated communication to determine if the received GRE encapsulated communication was received over an XCF link; and

means for discarding the received GRE encapsulated communication if the received GRE encapsulated communication was not received over an XCF link.

39. (Original) A computer program product for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which routes both inbound and outbound communications with target hosts which are associated with a secure network communication through the distribution processor; and

computer readable program code which processes both inbound and outbound secure network communications at the distribution processor so as to provide network security processing of communications from the target host and network security processing of communications to the target host.

40. (Original) A computer program product according to Claim 39, further comprising:

computer readable program code which receives at the distribution processor, network communications directed to the common network address; and

computer readable program code which distributes the received network communications to selected ones of the target hosts so as to distribute workload associated with the network communications.

41. (Original) A computer program product according to Claim 40, further comprising:

computer readable program code which determines if the received network communications are secure network communications which are to be distributed to ones of the target hosts;

wherein the computer readable program code which processes both inbound and outbound secure network communications at the distribution processor comprise computer readable program code which processes the received network communications so as to provide generic communications to the ones of the plurality of target hosts if the received network communications are secure network communications which are distributed to ones of the target hosts.

42. (Original) A computer program product according to Claim 41, wherein the computer readable program code which processes both inbound and outbound secure network communications further comprises:

computer readable program code which receives at the distribution processor communications from the ones of the target hosts which are associated with secure network communications; and

computer readable program code which processes the received communications from the ones of the target hosts so as to provide network security for the communications from the ones of the target hosts.

43. (Original) A computer program product according to Claim 42, wherein the communications received from the target hosts and the generic communications to ones of the plurality of target hosts are encapsulated in a generic routing format.

44. (Original) A computer program product according to Claim 42, wherein generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distributing processor and ones of the plurality of target hosts.

45. (Original) A computer program product according to Claim 42, wherein the communications received from the target hosts at the distribution processor and the generic communications to ones of the plurality of target hosts from the distribution processor are communicated over trusted communication links.

46. (Original) A computer program product according to Claim 42, further comprising the step of establishing common IP filters for communications encapsulated in the generic routing format at the distributing processor and the plurality of target hosts.

47. (Original) A computer program product according to Claim 46, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

48. (Original) A computer program product for providing Internet Protocol Security (IPSec) communications from a network to a plurality of application instances executing on a cluster of data processing systems utilizing virtual Internet Protocol Address (VIPA) Distributor to provide a routing communication protocol stack which distributes connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, the method comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which receives inbound IPSec communications to the DVIPA from the network at the routing communication protocol stack;

computer readable program code which performs IPSec processing of the received inbound IPSec communications at the routing communication protocol stack to provide non-IPSec communications to a first target communication protocol stack associated with the received inbound IPSec communications;

computer readable program code which receives outbound non-IPSec communications from a second target communication protocol stack at the routing communication protocol stack; and

computer readable program code which performs IPSec processing on the received outbound non-IPSec communications at the routing communication protocol stack to provide outbound IPSec communications to the network corresponding to the received outbound non-IPSec communications.

49. (Original) A computer program product according to Claim 48, wherein the target communication protocol stacks carry out the step of sending outbound communications associated with a connection utilizing IPSec which is routed through the routing communication protocol stack to the routing communication protocol stack for IPSec processing.

50. (Original) A computer program product according to Claim 47, further comprising:

computer readable program code which determining if an outbound communication associated with a connection utilizing IPSec is routed through the routing communication protocol stack;

computer readable program code which sending non-IPSec communications for the connection utilizing IPSec to the routing communication protocol stack if the connection utilizing IPsec is routed through the routing communication protocol stack; and

computer readable program code which IPSec processing communications if the connection utilizing IPSec is not routed through the routing communication protocol stack.

51. (Original) A computer program product according to Claim 48, where the routing communication protocol stack and the plurality of target communication protocol stacks communicate utilizing trusted communication link.

52. (Original) A computer program product according to Claim 51, wherein the cluster of data processing systems comprises a Sysplex and wherein the trusted communication link is a cross coupling facility of the Sysplex.

53. (Original) A computer program product according to Claim 47, further comprising:

computer readable program code which encapsulates the IPSec processed received IPSec communications in a generic routing encapsulation (GRE) formatted communication; and

computer readable program code which sends the GRE formatted communication to the first target communication protocol stack over a trusted communication link;

wherein the computer readable program code which receives outbound non-IPSec communications from a second target communication protocol stack at the routing communication protocol stack comprises computer readable program code which receives a GRE encapsulated communication from the second target communication protocol stack; and

wherein the computer readable program code performing IPSec processing on the received outbound non-IPSec communications at the routing communication protocol stack to provide outbound IPSec communications to the network corresponding to the received outbound non-IPSec communications comprises:

computer readable program code which extracts a non-IPSec communication from the received GRE encapsulated communication; and

computer readable program code which IPSec processes the extracted non-IPSec communication.

54. (Original) A computer program product according to Claim 53, further comprising computer readable program code which establishes common IP filters for GRE encapsulated communications at the routing communication protocol stack and the target communication protocol stacks.

55. (Original) A computer program product according to Claim 54, wherein the common IP filters bypass IP filtering for inbound GRE encapsulated communications.

56. (Original) A computer program product according to Claim 53, wherein the cluster of data processing systems comprises a Sysplex and wherein the routing communication protocol stack and the target communication protocol stacks communicate utilizing a cross coupling facility (XCF) of the Sysplex and wherein the GRE encapsulated communications include an XCF source address and an XCF destination address in an outer GRE header.

57. (Original) A computer program product according to Claim 56, further comprising:

computer readable program code which evaluates an IP address of a physical link over which a GRE encapsulated communication was received and an IP address in the received GRE encapsulated communication to determine if the received GRE encapsulated communication was received over an XCF link; and

computer readable program code which discards the received GRE encapsulated communication if the received GRE encapsulated communication was not received over an XCF link.